UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/710,691	11/09/2000	Henk J. Bots	21055-701	5696

2292 7590 12/03/2004

BIRCH STEWART KOLASCH & BIRCH
PO BOX 747
FALLS CHURCH, VA 22040-0747

EXAMINER	
BADERMAN, SCOTT T	

ART UNIT	PAPER NUMBER
2113	14

DATE MAILED: 12/03/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/710,691	Applicant(s) BOTS ET AL.	
	Examiner Scott T Baderman	Art Unit 2113	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 January 2002*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-11* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-11* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 November 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Objections

1. Claim 9 is objected to because of the following informalities: In lines 5, 14 and 16, "the public network" lacks antecedent basis. In lines 7 and 17, "public" should be "private". Appropriate correction is required.

Double Patenting

2. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and, *In re Thorington,* 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

3. Claims 1 and 9-11 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claim 4 of U.S. Patent No. 6,226,748. Although the conflicting claims are not identical, they are not patentably distinct from each other because patented claim 4 includes the limitations of a method for sending a first data packet from a first member of a virtual private network to a second member of the virtual private network, receiving the first data packet en route to the second member (destination address), determining (verifying) that the first data packet is being sent between members of the virtual private network,

determining the packet manipulation rules for packets sent between members of the virtual private network, forming a secure data packet (second packet) by executing the packet manipulation rules on the first data packet, forwarding the secure data packet (second packet) to the second member of the virtual private network (destination address), wherein the secure data packet contains information of a source address and a destination address of the first data packet (i.e., the second packet conceals the source and destination addresses), and wherein the ultimate source and destination addresses of the secure data packet being sent are concealed while in transit. However patented claim 4 does not specifically include the limitation of encapsulating the secure data packet in a second packet which identifies the source and destination addresses only for the virtual private network units.

A person skilled in the art would have understood that by generating a second packet by performing the packet manipulation rules on the first packet, and wherein the second packet conceals the source and destination address of the first packet, that this operation is similar to encapsulating the second packet.

With regard to the additional limitations in claim 4 of the patent, which are not included in claims 1 and 9-11 of the instant application, the omission of these limitations in claims 1 and 9-11 of the instant application is an obvious expedient since the remaining limitations in claim 4 of the patent perform the same function as the limitations in claims 1 and 9-11 of the instant application (*In re Karlson*, 136 USPQ 184 (CCPA 1963)).

4. Claim 6 is rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claim 4 of U.S. Patent No. 6,226,748. Although the conflicting claims are not identical, they are not patentably distinct from each other because

patented claim 4 includes most of the limitations of claim 6 of the instant application. The only limitation that patented claim 4 does not clearly include are the steps of receiving an encapsulated secure data packet and de-encapsulating the encapsulated secure data packet.

A person skilled in the art would have understood that by generating a second packet by performing packet manipulation rules on a first data packet, and generating a third packet by reversing the packet manipulation rules encompasses the process of encapsulating and de-encapsulating, respectively.

With regard to the additional limitations in claim 4 of the patent, which are not included in claim 6 of the instant application, the omission of these limitations in claim 6 of the instant application is an obvious expedient since the remaining limitations in claim 4 of the patent perform the same function as the limitations in claim 6 of the instant application (*In re Karlson*, 136 USPQ 184 (CCPA 1963)).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over Shwed et al. (WO 97/00471) in view of Lidinsky et al. (4,897,874) and Aziz et al. (5,548,646).

As in claim 1, Shwed discloses a method for sending a data packet from a first host to a second host through a virtual private network that comprises the steps of receiving the data packet en route to the second host, determining the packet manipulation rules for packets sent between the hosts through the virtual private network, forming a secure data packet by executing the packet manipulation rules on the data packet and forwarding the secure data packet to the second host through the virtual private network, wherein the secure data packet inherently contains information of a source address and a destination address of the secure data packet (Figures 5 and 16, Abstract, page 1: lines 27-29, page 2: lines 21-29, page 4: lines 6-27, page 5: lines 5-21, page 13: lines 10-12, page 14: lines 25-26, page 16: lines 3-26, page 22: lines 28-30, page 25: line 16-page 26: line 13). However, Shwed does not clearly disclose the steps of determining that the data packet is being sent between *members* of the virtual private network or wherein the ultimate source and destination addresses of the secure data packet being sent are concealed while in transit, by encapsulating the secure data packet, wherein the secure data packet includes an address portion and a data portion, in a second data packet which identifies the source and destination addresses only for the virtual private network units. Lidinsky discloses a method for protecting data transmitted in a virtual network from being accessed by unauthorized users outside of the network by determining that the data transmitted in the virtual network is being sent between members of the virtual network (Abstract, column 2: lines 3-6 and 56-63, column 3: lines 18-22). Aziz discloses a method for encapsulating a secure data packet in a second packet, wherein the ultimate source and destination addresses of the secure data packet being sent are concealed while in transit, and wherein the second packet only identifies the broadcast addresses of the source and destination networks (Abstract).

It would have been obvious to a person skilled in the art at the time the invention was made to include the step of determining that a data packet is being sent between *members* of a virtual private network into the method taught by Shwed above. This would have been obvious because Lidinsky clearly teaches that "it is important that the privacy between different networks be carefully protected *by ensuring that no user not a member of a particular network has access to data of that network*" (column 3: lines 18-22), which would lead a person skilled in the art to include the step of determining that the data packet taught by Shwed above is sent between *members* of the virtual private network so that security is ensured like that taught by Lidinsky above.

It would have also been obvious to a person skilled in the art at the time the invention was made to include the process of wherein the ultimate source and destination addresses of the secure data packet being sent are concealed while in transit, by encapsulating the secure data packet, wherein the secure data packet includes an address portion and a data portion, in a second data packet which identifies the source and destination addresses only for the virtual private network units into the method taught by Shwed and Lidinsky above. This would have been obvious because Aziz teaches that by encapsulating the secure data packet in a second packet the host identities are concealed, and an intervening observer can discern only the network identities (column 1: line 52 – column 2: line 36).

7. Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Shwed et al. in view of Lidinsky et al. and Aziz et al., as applied to claim 1 above, and further in view of Kirby et al. (5,828,846).

As in claim 2, Shwed, Lidinsky and Aziz disclose the method above. However, they do not clearly disclose a step of comparing source and destination addresses of a data packet to addresses stored in an address table in order to determine that the data packet is being sent between members of the virtual private network. Kirby discloses a method for controlling the passage of data packets via a virtual connection wherein source and destination addresses of the data packet are compared to addresses stored in an address table in order to determine whether passage of the data packet is valid (Figure 3, Abstract, column 1: lines 43-59, column 3: lines 4-11 column 4: lines 5-20).

It would have been obvious to a person skilled in the art at the time the invention was made to include a step of comparing source and destination addresses of a data packet to addresses stored in an address table in order to determine that the data packet is being sent between members of the virtual private network into the method taught by Shwed and Lidinsky above. This would have been obvious because Lidinsky clearly teaches that by determining that a data packet is being sent between *members* of a network, security is ensured that *no user not a member of a particular network has access to data of that network*, as was taught above, and Kirby clearly teaches that by comparing the source and destination addresses to a pre-stored address list in address table it can be determined whether the source and destination devices are valid to communicate with the data packet (column 4: lines 5-20), which is exactly what Lidinsky is trying to do. Based on the above teachings, a person skilled in the art would have been led to incorporate the teachings of Kirby into the method taught by Shwed, Lidinsky and Aziz above in order to determine that a data packet is being sent between *members* of a network since the method taught by Kirby will produce the results in which Lidinsky desires.

8. Claims 3-5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shwed et al. in view of Lidinsky et al. and Aziz et al., as applied to claim 1 above, and further in view of Wesinger, Jr. et al. (5,898,830).

As in claim 3, Shwed, Lidinsky and Aziz disclose the method above. Shwed further discloses methods that comprise algorithms, specifically encryption algorithms, to be utilized for data packets sent through the network (page 28: lines 17-26). However Shwed does not clearly disclose accessing a lookup table that maintains information identifying compression, encryption and authentication algorithms to be utilized for data packets sent through the network. "Official Notice" is taken that lookup tables are well known in the art and are commonly used to maintain information in which a user or device can access. Wesinger discloses a method for controlling the passage of information through a network wherein channel processing can be performed, wherein the channel processing may include encryption, compression and authentication algorithms (Abstract, column 11: lines 35-60).

It would have been obvious to a person skilled in the art at the time the invention was made to include a step of accessing a lookup table that maintains information identifying compression, encryption and authentication algorithms to be utilized for data packets sent through the network into the method taught by Shwed, Lidinsky and Aziz above. This would have been obvious because of the "Official Notice" statement made above and the teaching by Wesinger that channel processing is performed on data flowing through a communications channel to *enhance* some attribute of data, such as security, reproduction quality, etc. (column 11: lines 35-43), which would lead a person skilled in the art to incorporate the concept of

channel processing into the method taught by Shwed, Lidinsky and Aziz above since channel processing would actually provide an enhancement.

As in claim 4, Shwed, Lidinsky, Aziz and Wesinger disclose the method above. Further, Shwed discloses forming a secure data packet by encrypting *at least* a payload portion of the data packet and providing authentication information for the data packet (page 4: lines 10-12, 25-27 and 31-page 5: lines 1-21).

As in claim 5, Shwed, Lidinsky, Aziz and Wesinger disclose the method above. Further, Shwed discloses forming a secure data packet by concealing (encrypting) the source and destination addresses of the data packet according to the manipulation rules (page 4: lines 10-12 and 25-27, page 5: lines 27-30).

9. Claims 6 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shwed et al. (WO 97/00471) in view of Aziz et al. (5,548,646).

As in claim 6, Shwed discloses a method for recovering (decrypting) an original data packet from a secure data packet sent between members of a virtual private network that comprises the steps of receiving the secure data packet, determining the packet manipulation rules for packets sent between members of the virtual private network, recovering the original data packet by manipulating the secure data packet by reversing the identified packet manipulation rules and forwarding the recovered data packet to its destination, wherein the secure data packet inherently contains information of a source address and a destination address

of the secure data packet (Figure 16, page 4: lines 6-27, page 5: lines 5-30, page 13: lines 10-12, page 22: lines 28-30, page 25: line 16-page 26: line 13). However, Shwed does not disclose receiving an encapsulated secure data packet and de-encapsulating the encapsulated secure data packet. Aziz discloses a method for encapsulating a secure data packet in a second packet, wherein the ultimate source and destination addresses of the secure data packet being sent are concealed while in transit, and wherein the second packet only identifies the broadcast addresses of the source and destination networks (Abstract).

It would have been obvious to a person skilled in the art at the time the invention was made to include the process of wherein the ultimate source and destination addresses of the secure data packet being sent are concealed while in transit, by encapsulating the secure data packet, wherein the secure data packet includes an address portion and a data portion, in a second data packet which identifies the source and destination addresses only for the virtual private network units, and then de-encapsulating the encapsulated secure data packet upon it reaching its destination, into the method taught by Shwed above. This would have been obvious because Aziz teaches that by encapsulating the secure data packet in a second packet, the host identities are concealed, and an intervening observer can discern only the network identities (column 1: line 52 – column 2: line 36).

As in claim 9, Shwed discloses a system for securely exchanging data packets between members of a virtual private network group that comprises 1) a first computer (host 1) at a first site having a first network address, 2) a first router (inherently within the firewall 1) associated with the first site for routing data packets originating from the first computer over a public network, 3) a first virtual private network unit inherently disposed between the first router and

the public network, wherein the first virtual private network identifies virtual private network group data traffic and secures the data traffic by manipulating the data traffic according to packet manipulation rules maintained by the first virtual private network unit, 4) a second router (inherently within firewall 2) associated with a second site for coupling the second site to the public network, 5) a second virtual private network unit inherently disposed between the second router and the public network for intercepting network traffic destined for the second site, wherein the second virtual private network unit detects virtual private network group traffic and recovers original packet data and 6) a second computer at the second site having a second network address for receiving the packet data, wherein the data packet inherently contains information of a source address and a destination address of the data packet (Figure 16, page 4: lines 6-27, page 13: lines 10-12, page 22: lines 28-30, page 25: line 16-page 26: line 13). However, Shwed does not disclose wherein the ultimate source and destination addresses of the secure data packet being sent are concealed while in transit, by encapsulating the secure data packet, wherein the secure data packet includes an address portion and a data portion, in a second data packet which identifies the source and destination addresses only for the virtual private network units. Aziz discloses a method for encapsulating a secure data packet in a second packet, wherein the ultimate source and destination addresses of the secure data packet being sent are concealed while in transit, and wherein the second packet only identifies the broadcast addresses of the source and destination networks (Abstract).

It would have been obvious to a person skilled in the art at the time the invention was made to include the process of wherein the ultimate source and destination addresses of the secure data packet being sent are concealed while in transit, by encapsulating the secure data packet, wherein the secure data packet includes an address portion and a data portion, in a second

data packet which identifies the source and destination addresses only for the virtual private network units into the method taught by Shwed above. This would have been obvious because Aziz teaches that by encapsulating the secure data packet in a second packet, the host identities are concealed, and an intervening observer can discern only the network identities (column 1: line 52 – column 2: line 36).

10. Claims 7 and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shwed et al. in view of Aziz et al., as applied to claim 6 above, and in further view of Wesinger, Jr. et al..

As in claim 7, Shwed and Aziz disclose the method above. Shwed further discloses methods that comprise algorithms, specifically encryption algorithms, to be utilized for data packets sent through the network (page 28: lines 17-26). However Shwed does not clearly disclose accessing a lookup table that maintains information identifying compression, encryption and authentication algorithms to be utilized for data packets sent through the network. "Official Notice" is taken that lookup tables are well known in the art and are commonly used to maintain information in which a user or device can access. Wesinger discloses a method for controlling the passage of information through a network wherein channel processing can be performed, wherein the channel processing may include encryption, compression and authentication algorithms (Abstract, column 11: lines 35-60).

It would have been obvious to a person skilled in the art at the time the invention was made to include a step of accessing a lookup table that maintains information identifying compression, encryption and authentication algorithms to be utilized for data packets sent through the network into the method taught by Shwed and Aziz above. This would have been obvious because of the "Official Notice" statement made above and the teaching by Wesinger

that channel processing is performed on data flowing through a communications channel to *enhance* some attribute of data, such as security, reproduction quality, etc. (column 11: lines 35-43), which would lead a person skilled in the art to incorporate the concept of channel processing into the method taught by Shwed and Aziz above since channel processing would actually provide an enhancement.

As in claim 8, Shwed, Aziz and Wesinger disclose the method above, wherein Shwed further discloses that the source and destination addresses are modified (encrypted, concealed), wherein once the packet is decrypted (recovered), inherently, the source and destination addresses will also be decrypted (recovered) (page 4: lines 6-9, page 25: lines 16-26).

11. Claims 10 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shwed et al. in view of Aziz et al., as applied to claim 9 above, and further in view of Lidinsky et al..

As in claim 10, Shwed and Aziz disclose the system above. However, neither clearly disclose a means for verifying that the data packet is being sent between *members* of the virtual private network. Lidinsky discloses a system for protecting data transmitted in a virtual network from being accessed by unauthorized users outside of the network by determining that the data transmitted in the virtual network is being sent between members of the virtual network (Abstract, column 2: lines 3-6 and 56-63, column 3: lines 18-22).

It would have been obvious to a person skilled in the art at the time the invention was made to include the means for verifying that a data packet is being sent between *members* of a virtual private network into the system taught by Shwed and Aziz above. This would have been obvious because Lidinsky clearly teaches that "it is important that the privacy between different networks be carefully protected *by ensuring that no user not a member of a particular network has access to data of that network*" (column 3: lines 18-22), which would lead a person skilled in the art to include the means for verifying that the data packet taught by Shwed and Aziz above is sent between *members* of the virtual private network so that security is ensured like that taught by Lidinsky above.

As in claim 11, Shwed, Aziz and Lidinsky disclose the system above. Further, Shwed discloses forming a secure data packet by concealing (encrypting) the source and destination addresses of the data packet according to the manipulation rules (page 4: lines 10-12 and 25-27, page 5: lines 27-30).

Response to Arguments

12. Applicant's arguments with respect to claims 1-11 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

See form PTO-892.

14. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Scott T Baderman whose telephone number is (571) 272-3644. The examiner can normally be reached on Monday-Friday, 6:45 AM-4:15 PM, first Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Robert Beausoliel can be reached on (571) 272-3645. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Scott T Baderman
Primary Examiner
Art Unit 2113

STB